113/136-PLUSPAT-©Questel

Publication Stage
(A2) Application published without search report
Publication Stage 2
(A3) Search report
Publication Stage 3
(B1) Patent specification
Patent Number
EP1089516 A2 20010404 [EP1089516]
Patent Number 2
EP1089516 A3 20020828 [EP1089516]
Patent Number 3
EP1089516 B1 20061108 [EP1089516]
Title
(A2) Method and system for single sign-on user **access** to multiple web **servers**
French Title
(A2) Procédé et système pour donner l'accès à plusieurs serveurs par une seule transaction
German Title
(A2) Verfahren und Vorrichtung für authentifizierten Zugang zu einer Mehrzahl von Netzbetreibern durch eine einzige Anmeldung
Abstract
Methods and systems for single sign-on user **access** to multiple web **servers** are provided. A user is authenticated at a first web server (**e**.g., by user **name** and password). The first web server provides a web page to the user having a service selector (e.g., a hyperlink comprising the URL of a **second** web **server** offering the service indicated by the selector). When the user activates the service selector, the first web server constructs and transmits an encrypted authentication token (e.g., a cookie) from the first web **server** to a **second** web server via the user client. The first and **second** web **servers** share a sub-domain. The authentication token comprises an expiration time and is digitally signed by the first web server and is authenticated at the **second** web **server**. Upon authentication, the **second** web **server** allows the user to conduct a session at the **second** web **server**.
Application Nbr
EP00203266 20000920 [2000EP-0203266]
Priority Details
US15585399P 19990924 [1999US-P155853]
Inventor(s)
(A2) GRANDCOLAS MICHAEL L (US); LAW FRANCE (US); DOSHI ASHWIN (US); WILLIAMS MICHAEL (US); JANG YEONA (US); MERSCHEN TONI (US); PAN JACK (US)
Patent Assignee
(A2) CITICORP DEV CT INC (US)
Patent Assignee
Citicorp Development Center, Inc.; 12731 W. Jefferson Boulevard; Los Angeles, California 90066 (US)
Patent Assignee 2
(A3) CITICORP DEV CT INC (US)
Patent Assignee 3
(B1) CITICORP DEV CT INC (US)

1/1-EPBPAT-©EPO

Public. Number
EP1089516 B1 20061108 [EP1089516]
Claims (English)
1. A method of single sign-on user access to multiple web servers, comprising: authenticating a user (10) at a first web server (30), detecting a client request at said first web server (30), said first web server (30) determining a second web server (40) related to said request, creating an authentication token related to the user and transmitting said authentication token from the first web server (30) to the

user (10), and then from the user (10) to the second web server (40) in a Secure Socket Layer (SSL) session, authenticating the authentication token at the second web server (40); and allowing the user to conduct a session at the second web server (40), characterised in
that the authentication token is an encrypted single-use perishable token, which is digitally signed and given an expiration time by the first web server (30) wherein said expiration time is set to 20 minutes or less from the time at which the authentication token is created,
that said web servers (30, 40) maintain synchronized or correct clocks to examine the expiration time of the authentication token at the second web server (40) and allowing the user (10) to conduct a session at the second web server (40) only if the expiration time has not passed.
2. The method of claim 1, wherein the first web server (30) and the second web (40) server use a shared domain in common, to share information between themselves, wherein preferably the shared domain in common is established or designated as a common sub-domain.
3. The method of claim 2, wherein the authentication token comprises a cookie.
4. The method of claim 3, wherein authenticating the user (10) at the first web server (30) comprises receiving a user name and password.
5. The method of claim 4, wherein the first web server (30) and the second web server (40) comprise a federation of web servers.
6. The method of claim 5, wherein authenticating the authentication token at the second web server (40) comprises examining the cookie.
7. The method of claim 6, further comprising providing a web page to the user having a service selector, comprising a hyperlink.
8. The method of claim 7, wherein the hyperlink comprises a URL for the second web server (40).
9. A method of any preceding claim, for single sign-on user access to a federation of web servers.
10. The method of claim 9, further comprising allowing the user to conduct a session with the first web server (30).
11. The method of any preceding claim, further comprising confirming a match with the digital signature.
12. A system for single sign-on user access to multiple web servers, comprising: a means for authenticating a user at a first web server (30); a means for detecting a client request at said first web server (30), a means at said first web server (30) for determining a second web server (40) related to said request, creating an authentication token related to the user and transmitting said authentication token from the first web server (30) to the user (10), and then from the user (10) to said second web server (40) in a Secure Socket Layer (SSL) session, a means for authenticating the authentication token at the second web server (40); and allowing the user to conduct a session at the second web server (40), characterised by,
means for creating an encrypted single-use perishable token,
means for digitally signing the authentication token and giving it an expiration time by the first web server (30) arranged to set an expiration time of 20 minutes or less from the time at which the authentication token is created,
means for maintaining synchronized or correct clocks of said web servers (30, 40) for examining the expiration time of the authentication token at the second web server (40) arranged to allow the user (10) to conduct a session at the second web server (40) only if the expiration time has not passed.
13. The system of claim 12, the first web server (30) and the second web (40) server use a shared domain in common, to share information between themselves, and preferably the shared domain in common is established or designated as a common sub-domain.
14. The system of claim 13, wherein the authentication token comprises a cookie.
15. The system of claim 14, wherein the means for authenticating the user at the first web server (30) comprises means for receiving a user name and password.
16. The system of claim 15, wherein the first web server (30) and the second web server (40) comprise a federation of web servers.
17. The system of claim 16, wherein the means for authenticating the authentication token at the second web server (40) comprises means for examining the cookie.
18. The system of claim 17 further comprising a means in the form of a hyperlink for providing a web page to the user having a service selector.
19. The system of claim 18, wherein the hyperlink comprises a URL for the second web server (40).
20. A system according to any of claims 12-19 for single sign-on user access to a federation of web servers.
21. The system of claim 20 further comprising a means for allowing the user to conduct a session with the first web server (30).
22. The system according to any of claims 12-21 further comprising a means for confirming a match with the digital signature.

Claims (French)

1. Procédé pour donner l'accès à plusieurs serveurs web par une seule transaction, comprenant : l'authentification d'un utilisateur (10) au niveau d'un premier serveur web (30), la détection d'une requête client au niveau dudit premier serveur web (30), ledit premier serveur web (30) déterminant un deuxième serveur web (40) lié à ladite requête, créant un jeton d'authentification lié à l'utilisateur et transmettant ledit jeton d'authentification du premier serveur web (30) vers l'utilisateur (10), puis de l'utilisateur (10) vers le deuxième serveur web (40) dans une session à protocole SSL (Secure Socket Layer), l'authentification du jeton d'authentification au niveau du deuxième serveur web (40) ; et le fait de permettre à l'utilisateur de mener une session au niveau du deuxième serveur web (40), caractérisé en ce que le jeton d'authentification est un jeton périssable crypté à usage unique, qui est numériquement signé et auquel le premier serveur web (30) donne un temps d'expiration, ledit temps d'expiration étant fixé à 20 minutes ou moins à partir du moment où le jeton d'authentification a été créé, en ce que lesdits serveurs web (30, 40) maintiennent des horloges synchronisées ou correctes pour examiner le temps d'expiration du jeton d'authentification au niveau du deuxième serveur web (40) et permettant à l'utilisateur (10) de mener une session au niveau du deuxième serveur web (40) seulement si le temps d'expiration n'est pas passé.

2. Procédé selon la revendication 1, dans lequel le premier serveur web (30) et le deuxième serveur web (40) utilisent un domaine partagé en commun, pour partager des informations entre eux, dans lequel de préférence le domaine partagé en commun est établi ou désigné comme un sous-domaine commun.

3. Procédé selon la revendication 2, dans lequel le jeton d'authentification comprend un témoin de connexion (cookie).

4. Procédé selon la revendication 3, dans lequel l'authentification de l'utilisateur (10) au niveau du premier serveur web (30) comprend la réception d'un nom d'utilisateur et d'un mot de passe.

5. Procédé selon la revendication 4, dans lequel le premier serveur web (30) et le deuxième serveur web (40) comprennent une fédération de serveurs web.

6. Procédé selon la revendication 5, dans lequel l'authentification du jeton d'authentification au niveau du deuxième serveur web (40) comprend l'examen du témoin de connexion.

7. Procédé selon la revendication 6, comprenant en outre la fourniture d'une page web à l'utilisateur ayant un sélecteur de service, comprenant un lien hypertexte.

8. Procédé selon la revendication 7, dans lequel le lien hypertexte comprend une URL pour le deuxième serveur web (40).

9. Procédé selon l'une quelconque des revendications précédentes, pour donner l'accès à une fédération de serveurs web par une seule transaction.

10. Procédé selon la revendication 9, comprenant en outre le fait de permettre à l'utilisateur de mener une session avec le premier serveur web (30).

11. Procédé selon l'une quelconque des revendications précédentes, comprenant en outre la confirmation d'une correspondance avec la signature numérique.

12. Système pour donner l'accès à plusieurs serveurs web par une seule transaction, comprenant : un moyen pour authentifier un utilisateur au niveau d'un premier serveur web (30) ; un moyen pour détecter une requête client au niveau dudit premier serveur web (30), un moyen au niveau dudit premier serveur web (30) pour déterminer un deuxième serveur web (40) lié à ladite requête, créant un jeton d'authentification liée à l'utilisateur et transmettant ledit jeton d'authentification du premier serveur web (30) vers l'utilisateur (10), puis de l'utilisateur (10) vers ledit deuxième serveur web (40) dans une session à protocole SSL (Secure Socket Layer), un moyen pour authentifier le jeton d'authentification au niveau du deuxième serveur web (40) ; et le fait de permettre à l'utilisateur de mener une session au niveau du deuxième serveur web (40), caractérisé par

un moyen pour créer un jeton périssable crypté à usage unique,

un moyen pour signer numériquement le jeton d'authentification et lui donner un temps d'expiration par le premier serveur web (30) agencé pour fixer un temps d'expiration de 20 minutes ou moins à partir du moment où le jeton d'authentification a été créé,

un moyen pour maintenir des horloges synchronisées ou correctes desdits serveurs web (30, 40) pour examiner le temps d'expiration du jeton d'authentification au niveau du deuxième serveur web (40) agencé pour permettre à l'utilisateur (10) de mener une session au niveau du deuxième serveur web (40) seulement si le temps d'expiration n'est pas passé.

13. Système selon la revendication 12, dans lequel le premier serveur web (30) et le deuxième serveur web (40) utilisent un domaine partagé en commun, pour partager des informations entre eux, et de préférence le domaine partagé en commun est établi ou désigné comme un sous-domaine commun.

14. Système selon la revendication 13, dans lequel le jeton d'authentification comprend un témoin de connexion.

15. Système selon la revendication 14, dans lequel le moyen pour authentifier l'utilisateur au niveau du premier serveur web (30) comprend un moyen pour recevoir un nom d'utilisateur et un mot de passe.
16. Système selon la revendication 15, dans lequel le premier serveur web (30) et le deuxième serveur web (40) comprennent une fédération de serveurs web.
17. Système selon la revendication 16, dans lequel le moyen pour authentifier le jeton d'authentification au niveau du deuxième serveur web (40) comprend un moyen pour examiner le témoin de connexion.
18. Système selon la revendication 17, comprenant en outre un moyen sous la forme d'un lien hypertexte pour fournir une page web à l'utilisateur ayant un sélecteur de service.
19. Système selon la revendication 18, dans lequel le lien hypertexte comprend une URL pour le deuxième serveur web (40).
20. Système selon l'une quelconque des revendications 12 à 19, pour donner l'accès à une fédération de serveurs web par une seule transaction.
21. Système selon la revendication 20, comprenant en outre un moyen pour permettre à l'utilisateur de mener une session avec le premier serveur web (30).
22. Système selon l'une quelconque des revendications 12 à 21, comprenant en outre un moyen pour confirmer une correspondance avec la signature numérique.

Claims (German)

1. Verfahren für Benutzerzugang mit einmaliger Anmeldung zu mehreren Webservem, umfassend: Authentifizieren eines Benutzers (10) an einem ersten Webserver (30), Erfassen einer Client-Anforderung an dem ersten Webserver (30), wobei der erste Webserver (30) einen zweiten Webserver (40) bestimmt, auf den sich die Anforderung bezieht, Erzeugen eines Authentifizierungstokens, das sich auf den Benutzer bezieht, und UEbertragen des Authentifizierungstokens von dem ersten Webserver (30) an den Benutzer (10), und dann von dem Benutzer (10) an den zweiten Webserver (40) in einer Secure Socket Layer (SSL)-Sitzung, Authentifizieren des Authentifizierungstokens an dem zweiten Web -Server (40); und dem Benutzer gestatten, eine Sitzung an dem zweiten Webserver (40) auszuführen, dadurch gekennzeichnet,
dass das Authentifizierungstoken ein verschlüsseltes, begrenzt gültiges Token für einmalige Benutzung ist, welches digital signiert ist und dem von dem ersten Webserver (30) eine Ablaufzeit gegeben ist, wobei die Ablaufzeit auf 20 Minuten oder weniger von dem Zeitpunkt ab gesetzt ist, zu der das Authentifizierungstoken erzeugt wird,
dass die Webserver (30, 40) synchronisierte oder korrekte Uhren vorhalten, um die Ablaufzeit des Authentifizierungstokens an dem zweiten Webserver (40) zu überprüfen und es dem Benutzer (10) nur zu gestatten, eine Sitzung an dem zweiten Webserver (40) auszuführen, wenn die Ablaufzeit nicht verstrichen ist.
2. Verfahren nach Anspruch 1, wobei der erste Webserver (30) und der zweite Webserver (40) eine gemeinsame Domäne gemeinsam benutzen, um Informationen untereinander gemeinsam zu benutzen, wobei vorzugsweise die gemeinsam benutzte Domäne als eine gemeinsame Unterdomäne erstellt oder ausgewiesen wird.
3. Verfahren nach Anspruch 2, wobei das Authentifizierungstoken ein Cookie umfasst.
4. Verfahren nach Anspruch 3, wobei das Authentifizieren des Benutzers (10) an dem ersten Webserver (30) ein Empfangen eines Benutzernamens und eines Passworts umfasst.
5. Verfahren nach Anspruch 4, wobei der erste Webserver (30) und der zweite Webserver (40) einen Zusammenschluss von Webservern umfassen.
6. Verfahren nach Anspruch 5, wobei die Authentifizierung des Authentifizierungstokens an dem zweiten Webserver (40) ein UEberprüfen des Cookies umfasst.
7. Verfahren nach Anspruch 6, weiter umfassend ein Bereitstellen einer Webseite an den Benutzer, die eine Dienstauswahleinrichtung aufweist, umfassend einen Hyperlink.
8. Verfahren nach Anspruch 7, wobei der Hyperlink eine URL für den zweiten Webserver (40) umfasst.
9. Verfahren nach irgendeinem der vorhergehenden Ansprüche für Benutzerzugang zu einem Zusammenschluss von Webservern mit einmaliger Anmeldung.
10. Verfahren nach Anspruch 9, weiter umfassend, es dem Benutzer zu gestatten, eine Sitzung mit dem ersten Webserver (30) auszuführen.
11. Verfahren nach irgendeinem der vorhergehenden Ansprüche, weiter umfassend ein Bestätigen einer UEbereinstimmung mit der digitalen Unterschrift.
12. System für Benutzerzugang mit einmaliger Anmeldung zu mehreren Webservem, umfassend: Mittel zum Authentifizieren eines Benutzers an einem ersten Webserver (30); Mittel zum Erfassen einer Client-Anfrage an dem ersten Webserver (30), Mittel an dem ersten Webserver (30) zum Bestimmen eines zweiten Webservers (40), auf den sich die Anfrage bezieht, Erzeugen eines Authentifizierungstokens, das sich auf den Benutzer bezieht und UEbertragen des Authentifizierungstokens von dem ersten Webserver (30) zu dem Benutzer (10), und dann von dem Benutzer (10) zu dem zweiten Webserver

(40) in einer Secure Socket Layer (SSL)-Sitzung, Mittel zum Authentifizieren des Authentifizierungstokens an dem zweiten Webserver (40); und dem Benutzer zu gestatten, eine Sitzung an dem zweiten Webserver (40) auszuführen, gekennzeichnet durch

Mittel zum Erzeugen eines verschlüsselten, begrenzt gültigen Tokens für einmalige Benutzung,

Mittel zum digitalen Signieren des Authentifizierungstokens und um ihm durch den ersten Webserver (30) eine Ablaufzeit zu geben, eingerichtet, eine Ablaufzeit von 20 Minuten oder weniger von dem Zeitpunkt ab, zu der das Authentifizierungstoken erzeugt wird, zu setzen,

Mittel zum Vorhalten synchronisierter oder korrekter Uhren der Webserver (30, 40), um die Ablaufzeit des Authentifizierungstokens an dem zweiten Webserver (40) zu überprüfen, eingerichtet, dem Benutzer (10) zu gestatten, eine Sitzung an dem zweiten Webserver (40) nur auszuführen, wenn die Ablaufzeit nicht verstrichen ist.

13. System nach Anspruch 12, wobei der erste Webserver (30) und der zweite Webserver (40) eine gemeinsame Domäne gemeinsam benutzen, um Informationen untereinander gemeinsam zu benutzen, und vorzugsweise die gemeinsam benutzte Domäne als eine gemeinsame Unterdomäne erstellt oder ausgewiesen ist.

14. System nach Anspruch 13, wobei das Authentifizierungstoken ein Cookie umfasst.

15. System nach Anspruch 14, wobei das Mittel zum Authentifizieren des Benutzers an dem ersten Webserver (30) Mittel zum Empfangen eines Benutzernamens und eines Passworts umfasst.

16. System nach Anspruch 15, wobei der erste Webserver (30) und der zweite Webserver (40) einen Zusammenschluss von Webservern umfassen.

17. System nach Anspruch 16, wobei das Mittel zum Authentifizieren des Authentifizierungstokens an dem zweiten Webserver (40) Mittel zum UEberprüfen des Cookies umfasst.

18. System nach Anspruch 17, weiter umfassend ein Mittel in der Form eines Hyperlinks zum Bereitstellen einer Webseite an den Benutzer, die eine Dienstauswahleinrichtung aufweist.

19. System nach Anspruch 18, wobei der Hyperlink eine URL für den zweiten Webserver (40) umfasst.

20. System nach einem der Ansprüche 12 bis 19 für Benutzerzugang mit einmaliger Anmeldung zu einem Zusammenschluss von Webservern.

21. System nach Anspruch 20, weiter umfassend ein Mittel, um dem Benutzer zu gestatten, eine Sitzung mit dem ersten Webserver (30) auszuführen.

22. System nach einem der Ansprüche 12 bis 21, weiter umfassend ein Mittel zum Bestätigen einer UEbereinstimmung mit der digitalen Signatur.

Description

I. Cross Reference to Related Application

[0001] This patent application claims priority to co-pending United States Provisional Patent Application Serial No. 60/155,853, entitled "Method and System for Single Sign-On User Access to a Federation of Web Servers," filed September 24, 1999.

II. Field of the Invention

[0002] The present invention relates generally to the field of electronic commerce. More particular, embodiments of the present invention relate generally to a method and system for providing single sign-on user access to multiple web servers.

III. Background of the Invention

[0003] There are many situations in which an entity or group of entities, such as a global financial institution with banking, brokerage, and other aspects, wishes to combine the functional resources of different web application servers in order to aggregate functionality to the customers of the entity or group of entities. Such an entity or group of entities may wish to allow their customers access to such an aggregated functionality by signing on only once, by authenticating themselves once, and then being able to use different services which might be provided either by different servers of entities within the group of entities, or by servers of the group of entities and, for example, by servers of third party entities.

[0004] In this context, the entity or group of entities may wish to deliver to the customer, via a web browser, a set of services that are hosted by different web application servers. From an article "Secure attribute services on the web", J. S. Park, published in June 1999, there is known a method for single sign-on user access to multiple web servers which corresponds to what is defined in the preamble of claim 1. This known method, however, does show some deficiencies in relation to security and especially in relation to flexibility of the level of security dependent on what kind of session that is performed.

[0005] Moreover, such different web application servers may employ different platforms, such as a UNIX platform, an NT platform, or some other type of platform. The platform may have been constructed by different organizations within the group of entities, or the platform may have been provided by third-party providers. In any event, an essential problem is how to allow the customer to sign on once and then to redirect the customer to these different servers without requiring the customer to sign on each and every

time he or she goes accesses a different server.
[0006] Conventional products attempting to address this latter problem are deficient, for example, both in terms of performance and cost. In some such products, it is necessary to return to a centralized resource. Other such products do not support crossing organizational boundaries or Internet domain boundaries. According to a preferred embodiment there is a need for a methods and system for single sign-on user access to multiple web servers, such as a federation of web servers sharing sub-domains, that overcome such disadvantages and that provide other advantages.
IV. Summary of the Invention
[0007] The present invention provides methods and systems for single sign-on user access to multiple web servers, such as a federation of web servers sharing sub-domains, are provided. In an embodiment, a user is authenticated at a first web server (e.g., by user name and password). The first web server provides a web page to the user having a service selector (e.g., a hyperlink comprising the URL of a second web server offering the service indicated by the selector). Upon activation of the selector by the user, the first web server constructs, digitally signs, and transmits an encrypted authentication token (e.g., a cookie) from the first web server to a second web server via the user client. URL encoding is employed to encrypt and sign the authentication token. The first and second web servers share a sub-domain. The authentication token comprises an expiration time. The authentication token is examined and authenticated at the second web server and URL decoding is employed. Upon authentication, and if the expiration time has not passed, the second web server allows the user to conduct a session at the second web server.
[0008] In another embodiment, a method for single sign-on user access to a federation of web servers, such as a first and second web server sharing a sub-domain, is provided. In an embodiment, the method comprises allowing a user at a computing device to access a first web server in the federation of web servers via a web browser of the computing device, authenticating the user with user-provided authentication information, including at least a user identification, by the first web server, and allowing the user to conduct a session a the first web server. During the session, the first web server carries out the functions of prompting the user for selection of a functionality offered via at least a second web server, and receiving a selection by the user of the functionality offered via the second web server. Upon receiving a selection, the first web server creates an authentication token for the user including at least the user identification and with a pre-defined token expiry by the first web server, digitally signing (e.g., by public key encryption) the authentication token by the first web server. An embodiment further comprises qualifying the domain attribute of the authentication token with the shared sub-domain name by the first web server, sending the digitally signed authentication token to the web browser of the computing device by the first web server, redirecting the web browser to the second web server by the first web server, and sending the authentication token to the second web server by the web browser. The second web server decrypts the authentication token, confirms a match with the digital signature of the first web server, checks the pre-defined expiry of the authentication token by the second web server, and allows the user to conduct a session with the second web server if within the pre-defined token expiry.
[0009] In another embodiment, a method of single sign-on for multiple web servers, comprising receiving log-in data from a user in a first server, providing the user with a service selector, receiving an indication that the user selected the service selector, constructing an authentication token comprising profile data associated with the user, encrypting and signing the authentication token, redirecting the user to a second server, transmitting the authentication token to the user, receiving the authentication token in the second server, verifying the authentication token in the second server, and allowing the user access to a service provided by the second server. In one such embodiment, the authentication token comprises a cookie and further comprises expiration time data.
[0010] It is a feature and advantage of the present invention to provide a method and system for single sign-on user access to a federation of web servers that allows users already authenticated on a web site, such as a financial institution's web site, to have access, for example, to a service provider's web site without having to be re-authenticated via provision of a valid name and password.
[0011] To achieve the stated and other features and advantages, an embodiment of the present invention provides a method and system which enables single sign-on access for a user to a federation of web servers that allows user authentication at an entity's web site server, selection of a service provider URL, and passage of an authentication token by the entity's web site server to a service provider's server that contains sufficient information to enable the service provider's server, for example, to recognize the user as a valid service provider user and to provide the user with customer specific information.
[0012] Additional objects, advantages and novel features of the invention will be set forth in part in the description which follows, and in part will become more apparent to those skilled in the art upon examination of the following, or may be learned by practice of the invention.

V. Brief Description of Figures

[0013]

FIG. 1 shows an embodiment of a system according to the present invention.

FIG. 2 shows a flow diagram describing a process according to the present invention carried out in the system shown in FIG. 1.

FIG. 3 shows a visual depiction of web pages associated with web servers of the system shown in FIG. 1.

FIG. 4 shows a flow diagram describing an alternative process according to the present invention carried out in the system shown in FIG. 1.

VI. Detailed Description

[0014] FIG. 1 shows an embodiment of a system according to the present invention. A brokerage firm web server (BFWS) 30 includes a brokerage firm web site 32. The brokerage firm web server 30 (and likewise the brokerage firm web site 32) is in communication with the Internet 20. Likewise, a bank web server 40 includes a bank web site 42. The bank web server (BWS) 40 (and likewise the bank web site 42) is also in communication with the Internet 20. A customer 5 of both the brokerage firm and the bank is shown. The customer 5 has a user name and password to access both the brokerage firm web site 32 and the bank web site 42. The customer's personal computer 10 having a web browser such as Microsoft Internet Explorer or Netscape Navigator (a client) is in communication with the Internet 20 as well. The customer 5 uses the customer's personal computer and browser 10 to communicate with the web servers 30, 40 via the Internet. Herein, the term customer is used in many instances to indicate the client 10 as used by the customer. In addition to network communication facilities and other aspects, the brokerage firm web server 30 and the bank server 40 comprise programming to carry out the functions described herein.

[0015] FIG. 2 shows a flow diagram of steps carried out in the system shown in FIG. 1. The customer 10 points the customer's browser to the brokerage firm web site 32. The customer 10 logs into the brokerage firm web site 32 using the customer's correct user name (or user identification) and password for the brokerage firm web site 32, and is authenticated by the brokerage firm web server 30. Once the customer logs into the brokerage firm web site 32, the web site 32 presents the customer 10 with a welcome page from the web site 32. Once logged in, the customer 10 may examine the customer's brokerage account information, portfolio, investment information, and the like.

[0016] FIG. 3 shows a graphical depiction of the system shown in FIG. 1, including the welcome page 100 from the brokerage firm web site 30 provided to the customer 10 once the customer logs in at the brokerage firm web site 30. The welcome page 100 shown in FIG. 3 includes a service selector in the form of a hyperlink shown as "bill payment" 102. The brokerage web site offers its customers the ability to pay bills.

[0017] Referring again to FIG. 2, the customer 10 requests bill payment 50 by clicking on the "bill payment" hyperlink 102. The brokerage firm web server 30 itself does not handle the process of bill payment, but the server 30 is programmed with the knowledge that the bank web server 40 handles such a process. The hyperlink 102 includes the URL of the bank web site 42. Upon detecting the request of bill payment, the brokerage firm server 30 builds an authentication token 52. An authentication token comprises an object (or data) that can be passed between cooperating servers. A function of an embodiment of an authentication token is to convey the necessary information from a primary (or first) server to a secondary (or second) server to allow the secondary server to skip the sign-on process that would otherwise be necessary and required. Once a primary server establishes a session for a user, a cooperating secondary server that receives a valid authentication token from the primary server can establish a session without having the user sign on again.

[0018] In the embodiment shown in FIG. 1, the brokerage firm web server 30 builds an authentication token (or access token) comprising user identification data (or profile data) and expiration time data (token expiry) 52. The profile data comprises user identification data comprising a customer identification number that uniquely identifies the user to the secondary server. In the shown embodiment, the token also include a list of accounts of the customer. Expiration time data comprises data reflecting the time after which the authentication token is invalid. In the embodiment shown, the time is in Greenwich Mean Time (GMT). In other embodiments, the time may be in Universal Time. Expiration time may be set by the primary server at any desired time, though in most embodiments the expiration time is a relatively short time, e.g., three to twenty minutes, from the time at which the authentication token is created. In the embodiment shown, the expiration time is set at fifteen minutes from the time the authentication token is created. Note that it is important for the servers exchanging such authentication tokens to maintain correct or synchronized clocks. The use of expiration time is used to create a single-use, perishable token.

[0019] In the embodiment shown, the authentication token built comprises a cookie with profile data of the customer 5 and an expiration time of fifteen minutes from the creation time of the token.

Authentication tokens may also comprise URL strings or other data that may be passed between servers. The profile data of the customer includes a customer identification number for the customer 5. The brokerage firm web server 30 includes a data storage system (e.g., a hard disk drive) that has customer identification numbers associated with log-in user names used by customer's of the brokerage firm web server 30. These numbers were agreed upon previously by the administrators of the servers 30, 40. In the embodiment shown, a customer is associated with a customer identification number. In the embodiment, when the customer requests bill payment 50, the server 30 retrieves, from the data storage system, the customer identification number for the customer 5. This customer identification number retrieved is used in the profile data used to build the cookie 52.

[0020] In another embodiment, various customer identification numbers are associated with various secondary servers. When the customer requests a service provided at a secondary site (or to be transferred to a secondary site), the primary server detects the request, determines the secondary site, and retrieves, from the data storage system, the customer identification number for the requesting customer that is associated with the secondary site to which the customer will be directed for bill payment services.

[0021] Referring again to FIG. 2, the server 30 also selects the secondary server recipient name 54. The server 30 does so by examining the request made by the customer and determining the name / address of the appropriate secondary server to handle the request. In the embodiment shown, the server 30 examines the "bill payment" request made by the customer. In the present embodiment, the examination comprises determining the Uniform Resource Locator (URL) associated with the "bill payment" hyperlink. The web page file associated with the welcome page 100 includes the URL associated with the "bill payment" hyperlink, and the server 30 selects this URL.

[0022] The server 30 then signs and encrypts the cookie 56. A digital signature associated with the brokerage firm server 30 is applied to the cookie 56 by the server 30. Preferably, the server 30 comprises public key encryption software capable of encrypting, digitally signing, and authenticating electronic transactions across applications and servers. In the embodiment shown, the Entrust/PKI 5.0 software package, with its associated application programming interface (API) library, available from Entrust Technologies, Inc., Plano, Texas, is used to sign the cookie using a public key encryption system. In the embodiment shown, the cipher used is the Triple DES (Data Encryption Standard) encryption algorithm system, the encrypted cookie uses privacy-enhanced mail (PEM) headers, and signing uses the Secure Hash Algorithm (SHA-1) to create the message digest (or hash value) in signing. The Triple DES system is used to encrypt the authentication token (the cookie), and a PEM header and SHA-1 digest is included.

[0023] A digital signature associated with the server 30 (in the form of a signed-encrypted string) applied to the cookie allows a secondary server to verify that the authentication token was created by the brokerage firm server 30. Further, the signature allows a secondary server to detect any modification or corruption of the authentication token. The digital signature is applied and encrypted by the server 30.

[0024] In the embodiment shown, the cookie is created and kept on the browser 10 of the user 5 using a header entry in the response page, and the header entry is structured as follows: Set-cookie; name=value; expires=date-time; domain=domainname; path=path; secure. The path value comprises a specific directory, and the domainname value preferably is a common sub-domain (discussed further below). In an embodiment, the authentication token (the cookie) is non-persistent and will not be written to disk on the customer client 10. In such an embodiment, an expires value is not necessary, and the cookie will be deleted by the receiving server immediately after receipt.

[0025] An example of a string comprising cookie construction according to an embodiment of the present invention is as follows:

VER|1EXPDT|19990505132540.parallel.CTCUST|AF|EXIST.parallel.CID|57600100056005023
4.parallel.
FCID|0.parallel.TA|2.parallel.ANM|0010000001.parallel.RTN|099.parallel.ANA|My wife's
Checking.parallel.AB|237600.parallel.ANM|0010000002.parallel.RTN009.parallel.ANA|My
checking.parallel.AB|24556. The example is in the following format: Tag1 TagValue1 Tag2 TagValue2 Tag3 TagValue3 ....

[0026] It is noted that the specific tags and their tag values may vary according to implementation needs, such as destination server requirements.

[0027] Tags in the example shown, their value, and a description is shown in the following table:

(see table) [Unformatted table follows]

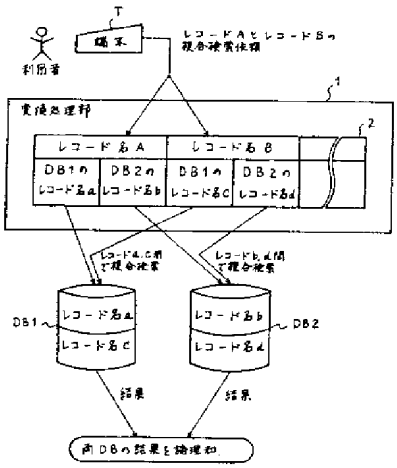
-- Tag Tag Value Description
-- VER 1 Version of cookie system being used (current version is 1)
-- EXPDT Date / Time The ASCII GMT date and time that the authentication token expires. Format: CCYYMMDDHHMMSS.
-- CT CUST FC Customer Type. CUST= regular customer. FC= Customer Representative. Used

to activate view-only mode.
-- AF NEW / EXIST New or existing customer indicator.
-- CID Integer Customer Identification Number
-- FCID Alphanumeric Identification number for customer service representative. If the user is a regular customer, do not set FCID (i.e., set to 0).
-- TA Integer Total Number of Accounts of customer
-- ANM Integer Account Number
-- RTN Integer Routing transit Number - maps to prod-type-cd
-- ANA Alphanumeric Account nick name
-- AB Integer Account Balance in cents (i.e. $10.50=1050)
End table
[0028] In the embodiment shown, the order of tags is not significant, except for ANM, ANA, AB, which are considered a tuple and are grouped together as shown above. Also, in the embodiment shown, the VER, EXPDT, and CT are required tags. Other tags that may be used in other embodiments include the following: AG (agency or corporation name that employs the user), FNAM (first name of user), and LNAM (last name of user).
[0029] The AF tag allows the bank server 40 to determine if an "Activate User" message should be sent to a transaction processing system (TPS). Preferably, if the brokerage firm web server 30 cannot determine whether a customer is new or already enrolled with GTPS, the server 30 sets the AF tag to NEW. In addition, the brokerage firm web server 30 shown assumes that all accounts are of the "Checking" type, and will set the product type code based on the RTN value determined.
[0030] The brokerage firm server 30 then URL encodes (also called URLEncode) the constructed cookie 58. Essentially, in URL encoding the cookie, the broker firm web server converts the formatted string discussed above to a URL-encoded format. In one embodiment, the URL encoding encodes the string using the URL escape syntax which comprises a three character string (%nn) specifying the hexadecimal code for a character. This syntax is used to hide characters that may be otherwise significant when used in a URL. The URL encoding 58 carried out by the brokerage firm web server 30 results in an encoded, signed, and encrypted string suitable for writing in a cookie, and such string is included in the cookie built by the server 30.
[0031] The brokerage firm web server 30 then sends a redirect command (or redirect page) with the URL encoded cookie (the authentication token) in a set-cookie header to the customer client 60. The redirect command includes the URL of the web site associated with "bill payment" 42. The customer client 10 receives the redirect command and the URL encoded cookie constructed by the brokerage web server 30.
[0032] The customer client 10 connects with the bank web site 42 via the Internet 20 and sends the cookie to the bank web server 62. In the embodiment shown, the authentication token is transmitted in a Secure Sockets Layer (SSL) session. Further, in the embodiment shown, on receipt of the redirect command, the customer client 10 opens a second browser window, requests a download of the home page at the URL of the web site 42 (or the page designated in the URL), receives the page of the web site 42 from the bank web server 40, and displays the page in the window. An embodiment of such a window 110 and page is shown in FIG. 3. The cookie received by the customer client 10 from the brokerage firm web server 30 is sent by the customer client 10 to the bank web server 40.
[0033] The bank web server 40 receives the cookie from the customer client 10. The bank web server 40 decodes the encoded, signed, and encrypted string built into the cookie by the brokerage firm web server 30 into a signed, encrypted string 64. Such decoding employs URL Decoding (or URLDecode) methods in the embodiment shown. In the embodiment shown, URL Decoding is employed to convert the URL encoded string in the cookie to plain ASCII for examination by the bank web server 40. The bank web server 40 and the brokerage firm web server 30 previously exchanged public-private key decryption information.
[0034] Once the string is decoded, the bank web server 40 decrypts and verifies the cookie (including the signed, encrypted string that is now decoded) 66. In the embodiment shown, software comprising public key encryption software capable of decrypting and authenticating electronic transactions across applications and servers is used by the bank web server 40 to do so. One example of such software is the Entrust/PKI 5.0 software package, with its associated application programming interface (API) library, available from Entrust Technologies, Inc., Plano, Texas.
[0035] The bank web server 40, using the software mentioned, determines whether the digital signature associated with the cookie verifies 68. If the signature does not verify, the bank web server 40 rejects the attempted sign-on and re-directs the customer client 10 to a web page on the brokerage firm web server 30 indicating an error and sign-on failure 70, resulting in a failed sign-on attempt 72. In another embodiment, if the signature does not verify, the bank web server 40 rejects the sign-on and sends a web page indicating an error and sign-on failure to the customer client 10. In an embodiment, if the

signature does not verify, the bank web server 40 also sends a message indicating such failure to the brokerage firm web site 30, e.g., an e-mail message.
[0036] If the signature verifies, the bank web server 40 examines the Certificate Authority (CA) name associated with the cookie 74. The server 40 compares the CA name associated with the cookie (i.e., the CA used with the CA name expected, as recorded in a registry file in the bank web server 40). If the CA name is not the one expected, the bank web server 40 re-directs the customer client 10 to an error page on the brokerage firm web server 70 and the sign-on attempt fails 72, as described above.
[0037] If the CA name is the CA name expected, the bank web server 30 next if the sender's name is correct 76. In doing so, the bank web server 30 determines whether the Common Name (CN) associated with the cookie (i.e., the name being certified - the name used by the brokerage firm web server 30) is an authorized name. In so determining, the bank web server 40 compares the CN associated with the cookie with a file containing authorized names in a data registry in the bank web server 40. If the CN is not the one expected, the bank web server 40 re-directs the customer client 10 to an error page on the brokerage firm web server 70 and the sign-on attempt fails 72, as described above.
[0038] If the CN is correct, i.e., if the CN is an authorized name, the bank web server 40 extracts profile data from the cookie and begins a bill-payment session 78. In the embodiment shown, the server 40 parses the clear text data associated with the cookie (clear text refers to the information that is not encrypted) 78, and examines the expiration time data in the cookie (not shown). If the expiration time has passed, the bank web server 40 re-directs the customer client 10 to an error page on the brokerage firm web server 70 and the sign-on attempt fails 72, as described above. The clear text data includes profile data (e.g., customer identification number). If the expiration time has not passed, the web server 40 begins a bill payment session using the session and profile data 78 by sending the customer client the web page 110 of the bank web site 42 that is shown in FIG. 3, and the sign-on is successful 80. The customer client 10 receives the web page 100 and proceeds with the bill-payment session with the bank server 40. In an embodiment, the authentication token (cookie) is then discarded or destroyed by the web server 40.
[0039] In an alternative embodiment, the system reflects a service associated with a user's employee. One such embodiment is shown in FIG. 4. In the embodiment shown in FIG. 4, the process of this alternative embodiment generally proceeds as that discussed above, with exceptions discussed below. The embodiment shown employs a primary server comprising a central web server having a central web site (not shown). The central web site comprises a web site at which the customer client 10 may request various services by clicking a hyperlink.
[0040] Referring to FIG. 4, the customer 5 signs on to the central web site 49, and the process 150, 152, 154, 156, 158, 160, 162, 164, 166, 168, 170, 174, continues in a manner like that described above in relation to steps 50, 52, 54, 56, 58, 60, 62, 64, 66, 68, 70, 74 shown FIG. 3, with the central web server serving as the primary server (the brokerage web server served as the primary web server in the embodiment shown in FIG. 2) until the step shown as item 77 occurs. The primary server includes the following, additional tags in the cookie: AG (agency or corporation name that employs the user), FNAM (first name of user), and LNAM (last name of user). The service provider referred to in FIG. 4 comprises the secondary server, and in the embodiment shown comprises the bank web server 40. After the bank web server 40 determines that the sender's CA is correct, the web server 40 determines whether the customer / user's employer has signed up with the service provider associated with the secondary server (the bank web server 40) 77. The bank web server 40 includes a database containing a list of employers who signed up with the service offered by the bank web server 40. The web server 40 compares the agency or corporation name in the AG tag with the list of employers. If the name in the AG tag is not on the list, the web server 40 re-directs the customer client 10 back to the central web site for an error URL 70.
[0041] If the name in the AG tag is on the list, the web server 40 continues the process by extracting profile data from the cookie and beginning a bill-payment session 78. After the bank web server 40 extracts profile data from the cookie and begins a bill-payment session 78, the server 40 examines a database (not shown) associated with the server 40 that includes data reflecting users who have previously signed up for or used the service provided by the server 40. If the user reflected by the cookie exists (i.e., has previously signed up for or used the service provided by the server 40), the web server 40 retrieves a default web page previously selected as the user's default page and sends the default web page to the customer client 83, and the customer client 10 then may proceed with a bill-payment session 80.
[0042] If the user reflected by the cookie does not exist (i.e., the database does not reflect that the user has previously signed up for or used the service provided by the server 40), the web server 40 creates a user identification using the tag information, including the AG, FNAM, and LNAM tag information, and stores the user identification in a database. The server 40 then retrieves a pre-designated default web page and transmits the web page to the customer client 83. The pre-designated default web page

comprises a pre-designated web page for users associated with the agency / corporation indicated in the AG tag. The customer client 10 then may proceed with a bill-payment session 80.
[0043] In an embodiment, multiple secondary servers are used in an embodiment of the present invention. In still other embodiments, multiple primary servers are used. A group of one or more primary and one or more secondary servers sharing log-in and other information as described herein may be referred to as a "federation" of servers.
[0044] In the embodiments shown herein, a digital certificate generation software program is used to generate certificates. An example of such software is the Entrust Solo Version 4.0 software package, available from Entrust Technologies, Inc., Plano, Texas. Preferably, when multiple secondary servers are employed in an embodiment of the present invention, the secondary servers will use the same profile (a file comprising information needed by the certificate before the server can authenticate). Also, preferably, the CN name in the profile matches the generic host name of the secondary server.
[0045] In embodiments, multiple primary servers are employed. The primary servers may use the same profile on all hosts or each host may use a separate profile. Like the secondary servers, certificates are employed in each primary server.
[0046] In an embodiment, servers sharing information between themselves that are maintained by different organizations use a shared domain in common in order to ease the sharing of information. In such an embodiment, a sub-domain is established or designated as the common sub-domain, the domain attribute of the authentication token (e.g., the shared cookie) is designated as the common sub-domain, and a "Forward IP (Internet Protocol) Pointer" entry is added in the DNS name servers of the cooperating organizations.
[0047] For example, the primary server sets a cookie sub-domain of xxxx.yyyy.com (wherein yyyy.com comprises the domain name of the primary server). Using "tail matching," cookies may be shared with any host whose domain tail is "yyyy.com." When the server searches a cookie list on the user's computer for valid or useable cookies, the server compares the domain attributes of the cookie with the Internet domain name of the host. If there is a tail match, then the cookie will go through path matching to see if it should be sent. "Tail matching" means that domain attribute is matched against the tail of the fully qualified domain name of the host. For example, a domain attribute of "xxxx.com" would match host names "yyyy.xxxx.com" as well as "zzzz.yyyy.xxxx.com." For example, the primary server with which the user interacts has a domain name of qqqq.yyyy.com, and the secondary server has a domain name of ssss.rrrr.yyyy.com, may share cookies in such an embodiment. In an embodiment, the IP pointer in the domain name server associated with the primary server either (1) maps the secondary server domain (ssss.rrrr.yyyy.com) to a pre-designated IP address associated with the secondary server; or (2) delegate the zone "rrrr" to a DNS name server associated with the secondary server for resolution.
[0048] As discussed above, certain embodiments of the present invention employ URL Encode and URL Decode. The following is a code fragment written in Microsoft C++ 6.0 showing an example of the implementation of URL Encode by a server: (see diagramm) (see diagramm)
[0049] The following code fragment shows the implementation of URL-Decode by as server: (see diagramm) (see diagramm)
[0050] Those of ordinary skill in the art will recognize that there are a variety of code fragments useful in carrying out such steps. Further, a variety of programming languages may be used.
[0051] Various embodiments of the invention have been described in fulfillment of the various objects of the invention. It should be recognized that these embodiments are merely illustrative of the principles of the present invention. Numerous modifications and adaptations thereof will be apparent to those skilled in the art without departing from the scope of the present invention.

135/136-PLUSPAT-©Questel



Publication Stage
(A) Doc. laid open to publ. inspec.

Patent Number
JP63071741 A 19880401 [JP63071741]

Title
(A) VIRTUAL **ACCESS SYSTEM** FOR **PLURAL** DATA BASES

Abstract
PURPOSE: To perform a composite retrieval between plural data bases by obtaining actual data base names and actual record **names** from **virtual** record names, to which a user designates, when a composite retrieval request which designates **virtual** record **names** is issued and performing composite retrieval at every obtained actual data base and returning OR results as an answer.
CONSTITUTION: The user designates **virtual** record **names** A and B from a terminal T and sends a composite retrieval request to a conversion processing part 1. In the conversion table 2 of the conversion processing part 1, a set of records indicated with the **virtual** record **name** A consists of records having a record name (a) in a data base DB1 and a record name (b) in a data base DB2, and a set of records indicated with the **virtual** record **name** B consists of records having a record name (c) in the data base DB1 and a record name (d) in the data base DB2. The conversion processing part 1 performs the composite retrieval between records (a) and (b) for the data base DB1 and performs that between records (b) and (d) for the data base DB2 and transfers OR between retrieval results from data bases DB1 and DB2 to the user. Thus, composite retrieval between plural data bases is performed with one retrieval request.
COPYRIGHT: (C)1988,JPO&Japio

Application Nbr
JP21686886 19860912 [1986JP-0216868]

Priority Details
JP21686886 19860912 [1986JP-0216868]

Inventor(s)
(A) NAKAGAMI KOSHIN; YAMADA MINEO; KAWANO SHIGEKAZU

Patent Assignee
(A) FUJITSU LTD; NIPPON TELEGRAPH & TELEPHONE

Patent Assignee
(A) FUJITSU LTD; NIPPON TELEGR & TELEPH CORP <NTT>